

January 22, 2009

Daniel Crane, Undersecretary
David Murray, General Counsel
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170
Boston, MA 02116

Top Priority: Protect Personal Information through Stakeholder Analysis

Dear Undersecretary Crane:

As leaders in business, the protection of personal information is a top priority and we write on behalf of a very broad range of businesses and industries that serve Massachusetts residents to express our deep concerns regarding many of the requirements of 201 CMR 17.00. While the delay in the effective date is helpful, it is unreasonable to believe, as a practical matter, that businesses or government agencies will have a fair opportunity to reach full compliance with these regulations as currently written. The requirements imposed by 201 CMR 17.00 set a difficult course for public and private entities, hindering our ability to invest and protect jobs in the Commonwealth. The Business Coalition urges the Patrick Administration to engage in a rigorous stakeholder analysis and to provide an opportunity for comment on the entire set of regulations within 201 CMR 17.00 so that the Department, Attorney General, regulated community and elected officials, can re-issue an entire set of rules by May 1, 2009, allowing for a two year period within which to implement the revised regulations.

As public policy matter, the business community supports laws and efforts aimed at protecting the personal information for residents of the Commonwealth. In fact, the business community demands that the successful implementation of regulations is necessary to protect personal information in the private and public sectors and to prevent further economic distress caused by the loss of personal data. However, regulations within 201 CMR 17.00 set a perilous course for already strained individuals, families, businesses and state agencies that depend upon the success and growth of the Massachusetts economy.

As currently written, 201 CMR 17.00 goes beyond the Legislature's intent through highly prescriptive mandates. For example, the Legislature never intended to make encryption mandatory. In many instances the regulatory mandates are not technically or economically feasible. Further, the regulations do not envision the national and global business relationships that Massachusetts firms depend on.

The implications of 201 CMR 17.00 will have a negative impact on "all persons" and all firms that conduct business in Massachusetts. In sharp contrast, the state of New Jersey is currently in the process of implementing their data security laws, which includes a process of more than two years just to promulgate regulations not including actual implementation periods.

Regrettably, the Massachusetts regulations do not provide similar time, clarity, recognition of federal regulations nor do they recognize the significant technological, legal, operational

challenges or the significant investments and human talent that many persons and small firms must now face. Today, “all persons” and firms regulated cannot achieve 100% compliance because these regulations ignore the fact that many of the technological, legal and operational requirements are not readily available to “all persons” or firms, regardless of readily available resources. The following is a partial list of the issues and solutions that the business community has identified:

Time: Is needed for collaborative stakeholder process with aggressive interaction by the Department, Attorney General, regulated community, and elected officials to develop revised rules. Compliance is an essential goal and this process will provide the best opportunity for regulated parties to understand and reach compliance.

Solution: The State of New Jersey is currently in a two year process just to promulgate a “pre-proposal” of regulations that do not yet specify actual implementation deadlines. In fact, on December 15, 2008, New Jersey issued its new pre-proposal after determining in April 2008 to reconsider and withdraw the proposed rules it had previously issued on April 16, 2007. New Jersey’s new pre-proposal provides for a comment period until February 13, 2009. Massachusetts regulations provide far less time. The regulations should be further refined and implemented in a phased manner to ensure the proper and appropriate level of education and outreach for the regulated community

Consistency: Is needed with existing and emerging federal law, and the laws of other states, to avoid duplication, wasted resources, confusion and undue complexity. The Massachusetts statute calls for uniformity and consistency with other laws, which is crucial for Massachusetts businesses and to ensure economic competitiveness. Moreover, there is no benefit to Massachusetts to impose unique requirements that merely conflict with or preempt other federal and state laws without providing any additional substantive protection for Massachusetts consumers, employees and other residents.

Solution: The Massachusetts statute requires consistency with federal law and as written these regulations place Massachusetts in an economic disadvantage. Last year Governor Patrick and Attorney General Coakley engaged in a regulatory review process to analyze and eliminate confusing, onerous and duplicative regulations. 201 CMR 17.00 is one of those very regulations, which that project set out to resolve.

Contract provisions and written certifications: Are duplicative, confusing, and unnecessary.

Solutions: A contract provision requirements should be used only. Contractual language should be used, not certification, and then on a going forward basis when contracts with third parties are newly created or renewed. Creating contractual provisions should be required of the first initiating party providing the personal data to the next third party so that each discrete data sharing event stands on its own. For example, party A would require a contract provision with party B when A shares personal data with B, but if B then shares the same data with another party then B has the obligation to require contractual provisions from the party it shares such data with. Each sharing would be a discrete contractual transaction. Without such discrete requirements, the contract requirement becomes a never ending, complex, costly, and circular

mandate virtually without end. For purposes of comparison, the recent New Jersey pre-proposal contains the following provisions with respect to third parties:

3. Review of service provider agreements by:

- i. Exercising appropriate due diligence in selecting service providers;
- ii. Requiring service providers to implement appropriate measures designed to meet the objectives of this sub-chapter; and
- iii. Taking appropriate steps to confirm that its service providers have satisfied these obligations, when indicated by the risk assessment of the business or public entity; and

Mandatory encryption: Is not mandated in the Massachusetts statute and its prescriptive nature negates the reasonableness standard within the statute.

Solutions: A principle or standard should be used allowing the regulated community to assure an outcome, rather than complying with a single command and control technology. Mandating a specific technique or technology undermines innovation and creativity, and it freezes in place old approaches. A single technology provides an easier target for theft than using a principle or result standard that invites innovative approaches, effective technologies, and flexibility to match circumstances. Inviting innovation by not locking in a single approach ensures that data holders will use up to date software, a concept required under the regulations, and will closely monitor systems.

Inventory: Requirements are complex and counterproductive, drawing resources away from more important objectives. Creating an inventory of the location of every personal data point is both unnecessary, resource debilitating and quickly becomes outdated.

Solutions: A better, more meaningful approach is to undertake a risk analysis of systems to identify the potential for the loss of such data as it moves. Risk analysis reveals strong and weak points of systems, identifies exactly where resources need to be focused to really protect data, and charts accountability. The risk assessment approach would be similar to what is required in other federal and state contexts.

Information collected and time held: Requirements are problematic and the regulatory structure does not require such regulations

Solutions: Personal data is an integral part of important global transactions today – in both the public and private sectors. Such data is used for important business, government and personal reasons. The scope of data held and time held are unconnected to breaches provided systems are vibrant and comprehensive – which is exactly what the statute requires subject to severe penalties (as well as destruction of the holder’s reputation). Restricting data collected and time held are redundant to the privacy requirements under the statute, and worse wastes resources and distracts focus from the primary goal of ensuring systems are protective of personal privacy.

Public sector: Needs to be held to exactly the same standards as the private sector. Personal data is regularly shared with public entities and is a source of significant data breaches.

Solutions: Unless the recipient public agency is held to the same standards and requirements as the private sector, the purpose of the statute is frustrated and rendered meaningless. Failure of the public sector to adhere to the same standards or requirements undermines public policy and makes a mockery of the statute's purpose.

Data security is not simple, no one person in a firm can provide the expertise and no one technological solution will provide security. The Business Coalition urges the Patrick Administration to provide an opportunity for greater stakeholder analysis with the Department, Attorney General, regulated community and elected officials. We must get this right – cost effective data privacy rules that comply with the statute, set standards, recognize existing programs, and invite innovation.

These comments represent but a few of the concerns the business community has with the Standards. Others include, but are not limited to: the Standards' encryption requirement that, for many businesses, will require abandoning existing systems and investing in completely new (and likely expensive) hardware and software that can accommodate encryption; the requirement to only provide electronic information in an encrypted form, which is impractical unless the recipient of such information – including the Commonwealth and its sister states are able and willing to accept encrypted information (which is not the case today); requiring the revision of all contracts with third-party vendors to ensure they include provisions expressly addressing data security; inconsistency with other state/Federal data security requirements; limitations on the use and maintenance of information; the costs associated with implementation; and the overly aggressive compliance date for implementing the Standards.

Therefore, industry experts and business leaders have aggressively identified issues and are committed to help the administration formulate and examine solutions for the successful implementation 201 CMR 17.00. We respectfully urge the administration to allow for this process, to re-issue an entire set of rules by May 1, 2009 with implementation of the rules over a two year period. Thank you for considering the long-term implications of these regulations for the protection of personal information of Massachusetts residents and the Massachusetts economy.

We appreciate your consideration of these concerns and strongly urge your assistance in working together with us on a solution, as New Jersey was able to accomplish by the Government and private sector working in tandem, to the above concerns that is in the best interest of the Commonwealth, its citizenry, and the business community.

Sincerely,

AeA
Affiliated Chambers of Commerce of Greater Springfield
American Insurance Association
American Rental Association of Massachusetts Inc.
American Staffing Association
Andover Country Club, Inc

AOL
Associated Industries of Massachusetts
Association of Independent Colleges and Universities in Massachusetts
AT&T
Avedis Zildjian Co.
Cambridge Chamber of Commerce
CitiGroup
Comcast
Consumer Data Industry Association
Costco Wholesale Corp.
CSW, Inc.
CTIA—The Wireless Coalition
First Data
Google
Greater Boston Chamber of Commerce
Greater Gardner Chamber of Commerce
Internet Alliance
Investment Companies Institute
Liberty Mutual
Life Insurance Association of Massachusetts
Massachusetts Marine Trades Association
Massachusetts Staffing Association
Massachusetts Association of Health Underwriters
Massachusetts Association of Insurance Agents
Massachusetts Bankers Association
Massachusetts Biotechnology Council
Massachusetts Business Roundtable
Massachusetts Council of Human Service Providers, Inc.
Massachusetts Food Association
Massachusetts High Technology Council & Defense Technology Institute
Massachusetts Hospital Association
Massachusetts Insurance Federation, Inc.
Massachusetts Mortgage Bankers Association
Massachusetts Package Store Association
Massachusetts Retail Lumber Dealers Association
Massachusetts Senior Care Association
Massachusetts Society of Certified Public Accountants
Massachusetts Technology Leadership Council
Mental Health and Substance Abuse Corporations of Massachusetts, Inc.
Metro South Chamber of Commerce
MetroWest Chamber of Commerce
Microsoft
Monster.com
National Federation of Independent Business/Massachusetts
National Retail Federation
New England Financial Services Association

North Central Massachusetts Chamber of Commerce
North Suburban Chamber of Commerce
Property Casualty Insurers Association of America
Reed Elsevier
Retail Industry Leaders Association
Retailers Association of Massachusetts
Rocky's Hardware
Securities Industry and Financial Markets Association
South Shore Chamber of Commerce
State Privacy and Security Coalition
Target Corporation
TechNet
The Gap
T-Mobile
Verizon
Walmart Stores, Inc.
Waltham West Suburban Chamber of Commerce
Worcester Regional Chambers of Commerce

Cc: Governor Deval Patrick
Lt. Governor Timothy Murray
Attorney General Martha Coakley
Speaker Salvatore DiMasi
President Therese Murray
Chairman Michael Morrissey
Chairman Michael Rodrigues
Secretary Daniel O'Connell
Gregory Bialeki, Undersecretary